Audit and Log Files – An Overview

V0.1 2021-11-25



Copyright © 2021 Real World Technology Solutions

All rights reserved.

Contents

[1 Audit and Log Files – An Overview 4](#_Toc88724124)

[1.1 Terminology 4](#_Toc88724125)

[1.2 Why Have Audit and Log Files? 4](#_Toc88724126)

[1.3 What Resources Should Have Audit and Log Files Enabled? 4](#_Toc88724127)

[1.4 When to Use Audit and Log Files 5](#_Toc88724128)

[1.5 Other Considerations 5](#_Toc88724129)

[2 Audit and Log Files Checklist 6](#_Toc88724130)

[2.1 Preparation 6](#_Toc88724131)

[2.2 Implementation 6](#_Toc88724132)

[2.3 Analysis and Review 6](#_Toc88724133)

# Audit and Log Files – An Overview

This document discusses audit and log files and their importance to protecting an organisation’s resources and its ability to maintain normal operations.

## Terminology

Some important definitions.

* Resources – a general term referring to IT systems, applications, networks, etc
* Audit File, Audit Log, Audit Trail – these three terms are generally used interchangeably to refer to the same type of file; the terms refer to a file that is used to record events, the cause or source of the events, and what the resource that experienced the events did in response to those events, if anything. (In this document, the term Audit File will be used.) Often these files are associated with resources that require some form of official audit from time-to-time; e.g. an accounting system or database may use Audit Files for legal as well as operational purposes
* Log File – sometimes also referred to simply as a Log; these types of files are similar in nature to Audit Files, except that they serve a more general use, including recording messages and information required for a particular purpose.

## Why Have Audit and Log Files?

These files provide information about the resources that generated them. That information is used for many purposes, including recording:

* Significant events, including the time of occurrence, event type, any information about the origin of the event, and other data that can characterise the event and its effects
* The resource’s response to recorded events, including any actions to manage the events automatically, or changes made to prevent potential actions stemming from the events from happening; e.g. if an attempt to access restricted data by an unauthorised account is detected, the file may record that the event occurred and the account was automatically suspended pending review by a person

The files can be analysed to:

* Monitor performance
* Detect normal and adverse events, including cyber security events
* Audit legitimate activities for legal or regulatory purposes
* Investigate breaches of “rules” (policies, legislation, regulations, etc)

The overall purpose of having these files is to be able to monitor and manage resources effectively.

## What Resources Should Have Audit and Log Files Enabled?

Each organisation should have its own policy on when to enable audit or log files. However, there are some basic principles that apply to all organisations:

* Understand the activities performed by all resources and decide if those activities need to be monitored for any reason
* Understand what monitoring is available for the resources needing to be monitored
* Decide what level of available monitoring is appropriate and understand what that monitoring will produce as well as its impact on the normal performance of the resource
* Understand what the information in the audit and log files means and decide how best to analyse and use that information
* Decide on the appropriate analysis process and, if relevant, analysis technology (e.g. the files will only be reviewed manually by people; the associated log file analysis software will be run and a report produced each day/week, etc)
* Implement the production and analysis of audit and log files
* Manage the audit and log files so that their production and usage is as desired (e.g. manage how large the files can grow, how their size is affecting storage, when to “roll” files and create new versions, when to delete files that are considered obsolete, etc)

This information informs decisions on what, when and where to produce and use audit and log files.

## When to Use Audit and Log Files

The whole purpose of producing audit and log files is to monitor resources and analyse the information produced to detect particular types of events and activities. Some general guidelines:

* If there are no explicit reasons to monitor a resource, do not produce audit or log files for it
* If monitoring is warranted, decide how much monitoring is appropriate – do not monitor more than is needed simply because it’s possible; only monitor that which will be genuinely useful and on which decisions will be made
* Sometimes monitoring may only be needed at specific times or during particular circumstances – if so, only monitor accordingly
* If the need for monitoring changes, review the production and use of audit and log files and adjust appropriately
* Weigh the benefits of detecting events and activities against any cost of monitoring (e.g. costs of software, impact on performance, effort time to implement, regular effort time to review, etc)

## Other Considerations

A useful approach to considering if and how to use audit and log files is to think of the SMART acronym:

* Specific – monitor for a purpose; there must be explicit reasons to monitor specific resources (e.g. monitor for repeated failed login attempts on the patient data system)
* Measurable – if it can’t be “measured” somehow, monitoring is useless. This means that the detection of the desired event or activity must be quantifiable in some sense, either by measured values, or countable items (e.g. more than three events of a certain explicit type is treated as a repeated attempt to perform an unauthorised action)
* Achievable – the available information must be able to be analysed to provide the desired result of the monitoring (e.g. detecting repeated failed logins is only useful if sufficient details of the attempts are available in the information so appropriate actions can be taken)
* Realistic – only monitor things that can be used to make decisions; if it cannot be used to make a decision that causes real-world actions, it probably should not be monitored (e.g. detecting failed login attempts by manually mapping connection information to a global database of suspected cyber attackers may be possible, but the substantial effort and time required may be unrealistic)
* Timely – Analysis and consequential decisions need to be done within timeframes that make them useful for effective outcomes (e.g. analysing once per month is not useful for detecting and responding to cyber security incidents)

# Audit and Log Files Checklist

This checklist can be used when deciding if the use of audit or log files is warranted for any resource.

## Preparation

* Purpose and nature of use of resource under consideration are well understood
* Reason for considering audit or log files on the resource is understood
* Policies, legislation and regulations requiring particular audit and log files are known and will be complied with
* Ability to produce and analyse audit or log files is known (e.g. software, people, etc)
* Information that can be collected in audit or log files is suitable for the purpose of monitoring for the identified purposes
* Specific information to be collected (and to be not collected) has been decided
* Costs of monitoring are known (e.g. financial (capital and operational), effort, time, etc)
* Benefits of monitoring are known and accepted as cost-effective
* Explicit decisions will be made based on analysed information
* Decision to proceed with monitoring confirmed or rejected

## Implementation

* Monitoring software is installed and usable (e.g. existing application, independent monitoring software, monitoring agent, etc)
* Monitoring software is configured to collect relevant data and not collect irrelevant data
* Analysis software installed and ready, and/or manual analysis processes defined
* Frequency of data collection and analysis determined and configured
* Monitoring and analysis commenced

## Analysis and Review

* Audit and/or log files being produced as expected
* Analysis occurring as expected
* Decisions being made according to analysis
* Audit and log files are being managed for size, rollover, deletion, etc
* Regular review of audit and log requirements being done (e.g. every 3 months, annually, etc)